PAT-NO: JP411066005A

DOCUMENT-IDENTIFIER: JP 11066005 A

TITLE: PASSWORD GENERATION DEVICE AND PASSWORD COMMUNICATION SYSTEM

PUBN-DATE: March 9, 1999

INVENTOR-INFORMATION:
NAME
ISHIKURA, HIROYUKI

ASSIGNEE-INFORMATION:
NAME COUNTRY
SHARP CORP N/A

APPL-NO: JP09227777

APPL-DATE: August 25, 1997

INT-CL (IPC): G06F015/00

ABSTRACT:

PROBLEM TO BE SOLVED: To input original data containing a feature for authentication with a simple input method and to generate a password by extracting a feature parameter from handwriting graphic information, executing a specified operation and converting it into a character string which can be read.

SOLUTION: Respective coordinate points in handwriting character string/ graphic information which are inputted are sampled by a coordinate point acquiring part 1-1 and a coordinate point normalization

part 1-2 executes
normalization. They are outputted to a feature parameter extraction part 1-3.
A block operation part 1-4 considers the inputted feature parameter as a bit
stream, divides it, into blocks at every n-blocks, executes an operation for
respective groups and outputs them to a password generation part 1-5 as
password parameters. The password generation part 1-5 segments the inputted
password parameters at every m-bits, consults a dictionary table 1-6 with the
password parameter as an index and outputs data obtained by connecting all the
outputs of a dictionary at every m-bits as the password.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－66005

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ

審査請求　未請求　請求項の数８　ＯＬ　（全６頁）

(21)出願番号　特願平9－227777

(22)出願日　平成９年(1997)８月25日

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号

(72)発明者　石倉　裕之
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

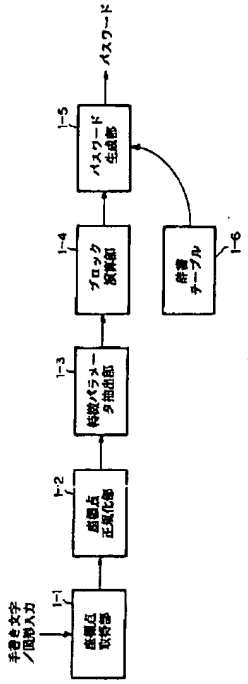
(74)代理人　弁理士　高野　明近　（外１名）

(54)【発明の名称】　パスワード生成装置及びパスワード通信システム

(57)【要約】

【課題】　簡単な入力方法で認証用の特徴を含む元データを入力し、入力された元データの特徴を損なうことなく、また、既存の情報処理装置に適応することができ、さらに、通信網を通して送信システムへも適応することができるようなデータ処理をしてパスワードを生成するための装置及び該装置をシステム要素とする通信システムを提供する。

【解決手段】　手書き文字・図形情報から座標点を座標点取得部１－１で取得し、この座標点に基づき抽出した特徴パラメータからブロック演算部１－４で一方向性ハッシュ関数アルゴリズムを用いパスワードパラメータを生成し、このパラメータのビットストリームをインデックスとして辞書テーブル１－６を用いることでパスワードを生成して個人認証に利用する。



1

【特許請求の範囲】

【請求項1】　任意の文字・図形を表わす座標信号を出力する文字・図形入力手段と、該文字・図形入力手段から出力される座標信号をサンプリングし正規化を行う座標データ処理手段と、該座標データ処理手段から出力され正規化された座標データが表現する文字・図形から特徴パラメータを抽出する特徴パラメータ抽出手段と、該特徴パラメータ抽出手段から出力される特徴パラメータをビットストリームとみなして演算する演算処理手段と、辞書テーブルと、前記演算処理手段からの演算結果により前記辞書テーブルを用いてパスワードを生成するパスワード生成手段を備えることを特徴とするパスワード生成装置。

【請求項2】　請求項1記載のパスワード生成装置において、前記演算処理手段の演算を特徴パラメータの前記ビットストリームの所定ビットの処理ブロック単位で行うことを特徴とするパスワード生成装置。

【請求項3】　請求項1又は2記載のパスワード生成装置において、前記演算処理手段の演算に一方向性ハッシュ関数を用いることを特徴とするパスワード生成装置。

【請求項4】　請求項1ないし3のいずれかに記載のパスワード生成装置において、前記辞書テーブルのインデックスとして前記演算処理手段から求められるパスワードパラメータを用いることを特徴とするパスワード生成装置。

【請求項5】　請求項4記載のパスワード生成装置において、前記演算処理手段の演算結果である前記パスワードパラメータを所定のビット単位に区切り、区切られた該単位それぞれのブロックの値をインデックスとして前記辞書テーブルを参照してパスワード列を取得することを特徴とするパスワード生成装置。

【請求項6】　請求項1ないし5のいずれかに記載のパスワード生成装置において、前記文字・図形入力手段として任意の文字・図形の入力操作に伴って生じる作用力を出力信号として発生させるものとし、該出力信号を前記特徴パラメータに反映させることを特徴とするパスワード生成装置。

【請求項7】　請求項1ないし6のいずれかに記載のパスワード生成装置において、前記文字・図形入力手段として、タブレット・タッチパネルなどを用いることを特徴とするパスワード生成装置。

【請求項8】　請求項1ないし7のいずれかに記載のパスワード生成装置を備える通信端末と、前記パスワード生成装置により生成されて、前記通信端末より送信されてくる前記パスワードを受信し、得た該パスワードをチェックする手段を備える他の通信端末とをシステム要素として構成されるパスワード通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、手書き図形入力手段で代表される任意の文字・図形を入力する手段として用いることができる情報端末と、情報の入出力・通信・格納等を行う情報処理装置が、通信網で接続されている場合において、情報処理装置が携帯端末の利用者を通信網経由で認証するのに用いるパスワード生成装置及びパスワード通信システムに関する。

2

【0002】

【従来の技術】従来、通信網経由で情報処理装置間の認証を行う場合、数文字～数十文字の文字列をパスワードとして送ることで認証を行うことが多い。すなわち遠隔地側の情報処理装置を利用するときは、自分側の端末のキーボードを利用してパスワード入力を行い、入力したパスワードを通信網を通して送り、事前に登録してあったパスワードとの比較を遠隔地の情報処理装置が行い、両者が一致していれば利用可能とする形態である。また、S／keyなどの使い捨てパスワードを利用する手段があり、これには数文字からなる英単語を数語から十数語連ねた文字列（パスフレーズ）を元に、使い捨てパスワードを生成し、これを送ることで認証を行う。

【0003】また、従来、手書き入力の端末でパスワードを入力する場合、一字一字手書き文字認識を行わせて入力するか、端末の画面上に表示された文字を選択することによって文字を入力する方式などを利用している。既存の手書き入力された図形を利用して個人認証を行う技術としては、特開平7－262372号公報がある。この技術では手書き図形から座標点をサンプリングし正規化した後に、特徴パラメータを計算し、特徴パラメータそのものをパスワードとして比較することで認証を行う。また、計算機のオペレーティングシステムによるパスワードを用いる認証技術は数多く存在する。

【0004】

【発明が解決しようとする課題】認証の確実性を高く保つにはパスワード列は長い方がいいが、手書き文字認識による入力や、画面上に表示された文字を選択する方式での入力では、長いパスワード列を入力するのは手間がかかるし、正しい入力を行うことは、困難である。また、さらに安全性の高い使い捨てパスワード技術を利用するには、英単語数語～数十語を入力することが必要となり、さらに入力は困難になる。また、コンピュータが遠隔地にあり、ネットワーク経由で認証を行う場合には、認証のために送るパラメータのデータ量が問題となる。特開平7－262372号公報の技術は、ネットワーク経由で認証を行うことを考慮してはいないが、そのままの形で認証の主体を遠隔地のコンピュータに移してネットワーク経由での認証に利用するような場合、手書き図形の特徴パラメータがネットワーク上を流れることになる。手書き図形の特徴パラメータは一般にはデータ量が大きく、そのままネットワーク経由の認証に用いるのには適さない。座標点の正規化の目を荒いものとすればデータ量は小さくなるが、特徴パラメータとしての性

質は弱くなり、認証に用いるのには適さなくなってしまう。また、特徴パラメータ同士の比較による認証を行うためには、手書き入力の端末でアクセスする可能性のある全コンピュータの認証システムを対応するものに入れ替える必要があり、システム入れ替えのコストが問題となる。

【０００５】本発明は、上記従来技術における問題点に鑑みてなされたもので、簡単な入力方法で認証用の特徴を含む元データを入力し、入力された元データの特徴を損なうことなく、また、既存の情報処理装置に適応することができ、さらに、通信網を通して送信システムへも適応することができるようなデータ処理をしてパスワードを生成するための装置及び該装置をシステム要素とする通信システムを提供することを解決課題とする。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明は、任意の文字・図形を表す座標信号を出力する文字・図形入力手段（手書き入力手段）を持つ情報端末において、前記文字・図形入力手段で入力された手書き図形情報から特徴パラメータを抽出し、抽出された特徴パラメータに対して一方向性ハッシュ関数を通すなどのある種の演算を行なった後に可読な文字列に変換することで、従来のネットワーク経由の認証方式で利用できるパスワードに変換する手法を特徴とする。ここで、一方向性ハッシュ関数とは、暗号理論入門（岡本栄治著，共立出版）にあるとおり、衝突を起こしにくい圧縮関数ｈのことである。衝突とは異なるｘ，ｙに対してｈ（ｘ）＝ｈ（ｙ）となることであり、圧縮関数とは、任意ビット超のビット列をある長さのビット列に変換する関数である。特徴パラメータが最終的には既存のシステムのパスワードとして利用できるものに変換されるので、認証システムを入れ替える必要がない。また、前記方法によって得られるパスワードのデータ量は数文字～数十文字程度であり、一般に考えられる特徴パラメータのサイズより充分に小さいため、認証に必要なネットワーク資源が小さくて済み、低速な回線を経由する場合でも利用することが可能となる。

【０００７】ここに、特徴パラメータからパスワードの変換に際する情報量の減少によって、パスワードの安全性が下がるように見えるが、前記演算方法を一方向性の高いものとすれば、本発明によって生成されたパスワードが他のパスワードと偶然一致する可能性が無視できるほど低くなるため、従来のキーボード入力によるパスワードの安全性と同程度の安全性は確保できる。

【０００８】また、本方式によって手書き情報からパスワードへの変換を行えば、既存のネットワーク環境に存在する各コンピュータの認証システムを入れ替えることなく、新たに手書き図形入力手段を持つ情報端末を既存のネットワーク環境に追加することが可能となる。さらに、特徴パラメータから変換して得られた可読文字列は、見た目の有意性を持たないため、辞書探索によるパスワードへの攻撃に対して強くなり、パスワードの安全性が高い。

【０００９】そして、各請求項記載の発明は、上記課題を解決する技術手段として下記を構成する。請求項１の発明は、任意の文字・図形を表わす座標信号を出力する文字・図形入力手段と、該文字・図形入力手段から出力される座標信号をサンプリングし正規化を行う座標データ処理手段と、該座標データ処理手段から出力され正規化された座標データが表現する文字・図形から特徴パラメータを抽出する特徴パラメータ抽出手段と、該特徴パラメータ抽出手段から出力される特徴パラメータをビットストリームとみなして演算する演算処理手段と、辞書テーブルと、前記演算処理手段からの演算結果により前記辞書テーブルを用いてパスワードを生成するパスワード生成手段を備えることを特徴としたものである。

【００１０】請求項２の発明は、請求項１の発明において、前記演算処理手段の演算を特徴パラメータの前記ビットストリームの所定ビットの処理ブロック単位で行うことを特徴としたものである。

【００１１】請求項３の発明は、請求項１又は２の発明において、前記演算処理手段の演算に一方向性ハッシュ関数を用いることを特徴としたものである。

【００１２】請求項４の発明は、請求項１ないし３いずれかの発明において、前記辞書テーブルのインデックスとして前記演算処理手段から求められるパスワードパラメータを用いることを特徴としたものである。

【００１３】請求項５の発明は、請求項４記載の発明において、前記演算処理手段の演算結果である前記パスワードパラメータを所定のビット単位に区切り、区切られた該単位それぞれのブロックの値をインデックスとして前記辞書テーブルを参照してパスワード列を取得することを特徴としたものである。

【００１４】請求項６の発明は、請求項１ないし５のいずれかの発明において、前記文字・図形入力手段として任意の文字・図形の入力操作に伴って生じる作用力を出力信号として発生させるものとし、該出力信号を前記特徴パラメータに反映させることを特徴としたものである。

【００１５】請求項７の発明は、請求項１ないし６のいずれかの発明において、前記文字・図形入力手段として、タブレット・タッチパネルなどを用いることを特徴としたものである。

【００１６】請求項８の発明は、請求項１ないし７のいずれかに記載のパスワード生成装置を備える通信端末と、前記パスワード生成装置により生成されて、前記通信端末より送信されてくる前記パスワードを受信し、得た該パスワードをチェックする手段を備える他の通信端末とをシステム要素として構成されたものである。

【００１７】

5

【発明の実施の形態】本発明についての一実施例に関して図面を参照して説明する。図1は、本発明によるパスワード生成装置の一実施例をブロック図で示すもので、この実施例においては図示しない外部の手書き文字列・図形入力部によって入力された手書き文字又は文字列および図形からパスワードを生成する。ここでいう手書き文字列・図形入力部としては、例えば、入力ペンと描画ボードを有し、ペンを用いて描画ボードに手書き文字・図形を書くことによって手書き文字・図形を入力することができる周知の手書き文字・図形入力装置や、タッチパネルのような入力ボード上に指などで手書き文字・図形を書くことで手書き文字・図形を入力することができる手書き文字・図形入力装置などの周知の装置から構成できる。前記手書き文字列・図形入力部で入力された手書き文字列・図形情報は、座標点取得部1－1へ入力され、座標点取得部1－1は各座標点をサンプリングし、結果を座標点正規化部1－2に出力する。

【0018】座標点正規化部1－2では、サンプリングされた座標点の正規化を行い、正規化された座標点を特徴パラメータ抽出部1－3へ出力する。ここでの正規化とは、簡単には描画ボード上の絶対座標で表現されている座標点を、手書き開始点を座標（0，0）とした相対座標に直し、座標をある程度の幅を持たせて丸め込むようなものである。この正規化によって、入力ごとの手書き座標のずれによる特徴パラメータの変化を小さく押さえることが可能となる。特徴パラメータ抽出部1－3では、正規化された座標をもとに特徴パラメータを抽出し、得られた特徴パラメータをブロック演算部1－4へ出力する。ここで、特徴パラメータとは入力された文字・図形の特徴を示すものである。たとえば、タブレット・タッチパネルなどで入力された座標情報にサンプリングと正規化を行い、得られた座標列を、次の座標点の差分を列としてならべて符号化したものを特徴パラメータとして利用することができる。

【0019】ブロック演算部1－4では、入力された特徴パラメータをビットストリームと見なしてnビット毎のブロックに分割し、それぞれのグループに対して演算を行う。そして各ブロックの演算結果を結合したものをパスワードパラメータとし、パスワード生成部1－5へ出力する。ここでブロック長nは特徴パラメータの大きさ，ブロック演算部1－4で用いられる演算方法，パスワード生成部1－5で用いる辞書テーブル1－6の引き方，最終的に出力されるパスワードの長さの4つによって決まる。演算として一方向性ハッシュ関数アルゴリズムの一つであるMD5アルゴリズム（R.Rivest:The MD5 Message-digest algorithm, Network Working Group, Request for Comment 1321)を用いた場合の例を図2に示す。なお、ここではブロック長nを1024としている。

【0020】ブロック演算部1－4では、図2に示すように、入力された特徴パラメータをビットストリームと見なし、1024ビット毎に切り出し（2－1）、切り出されたブロック単位でMD5を通して演算を行い（2－2）、演算結果を128ビットで出力し、ビットストリームとして再び接続したものをパスワードパラメータ列とする。MD5のように一方向性が高い関数の場合、異なる入力で同じ出力を得るのが困難なため、出力のパスワードパラメータの一意性は高く保たれたままとなる。ここでは、MD5の出力は128ビットであるため、ブロック長nを128より十分大きくとらなければデータ量削減の効果が出ない。また、入力の特徴パラメータのビット長が比較的短い場合（例えば、512ビット）はn＝256のようにブロック長nを小さ目にとると、最終的なパスワード長を長くとれる。

【0021】パスワード生成部1－5（図1参照）では、入力されたパスワードパラメータをmビット毎に区切り、区切られたビットストリームをインデックスとして辞書テーブル1－6を引き、辞書の出力を得る。そして、パスワードパラメータの各mビット毎の辞書の出力すべてを接続したものをパスワードとして出力する。ここで、mは、mビットの数値の最大値が辞書テーブル1－6のサイズと等しくなるように選ばれる。図3に、m＝16としたパスワード生成部1－5で行われるパスワード生成の具体例を示す。図3において、パスワード生成部1－5で入力されたパスワードパラメータ列をビットストリームと見なし、16ビット毎で切り出す（3－1）。得られた16ビット長のビットストリームを整数値と見なし、これをインデックスとして英単語辞書テーブル3－3を引く（3－2）。英単語辞書テーブル3－3を引いて得られた英単語を文字又は文字列として接続して最終的なパスワード列を生成する。

【0022】英単語辞書テーブル3－3の内容が文字であれば、得られるパスワードは数文字の文字列（上記したMD5の例では8文字の文字列）となり、一般的な認証に利用されるパスワードとして利用できる。図4は、パスワードパラメータからパスワードを生成するプロセスを示す図で、パスワードパラメータのビット列を整数値の列とみなし、整数値（1，26，25，2，51）に対応してこの例では文字の辞書テーブルを参照し、（aAzbZ）をパスワードとして得る。

【0023】また、辞書テーブルの内容が英単語であれば、得られるパスワードは数語～十数語となり、使い捨てパスワードを生成する元となるパスフレーズとして利用できる。図5は、パスワードパラメータからパスワードを生成するプロセスを示す図で、パスワードパラメータのビット列を整数値の列とみなし、整数値（1，20，98，0）に対応して、この例では、単語の辞書テーブルを参照し、(abate flower zymurgy abandon)をパスワードとして得る。図6は、本発明の一実施例をブロック図で示すもので、パスワード生成装置を備える通

信端末と、前記パスワード生成装置が生成したパスワードをネットワーク（例えば、秘密性を保証されない公衆回線）経由で受信し、得たパスワードをチェックする通信装置とを備えるパスワード通信システムの例である。

【００２４】

【発明の効果】

請求項１に対応する効果：長いパスワードを入力するのと等価な結果を、簡単な手書きによる図形入力で行うことができる。入力図形がもつ特徴パラメータをその特徴を反映した特徴パラメータより短いビットストリームのパラメータに変換し、さらに辞書テーブルを用いて可読文字列のパスワードに変換することで、特徴パラメータの唯一性を高く保持したまま可視文字列への変換が可能となる。よって、特徴パラメータをより短いパスワード列をやりとりすることで特徴パラメータそのものでやりとりすると同等の効果を得られ、パスワードの認証処理手段への負荷が減少する。また、変換後の可読文字列を、既存の認証システムのパスワードに利用している形式と同じ物とすることが可能であり、ソフトウェアを変更することなく既存のシステムに導入可能となる。

【００２５】請求項２に対応する効果：請求項１に対応する効果に加えて、特徴パラメータの唯一性を高く保持したままより短いビットストリームのデータに変換する演算処理を簡素化することができる。

【００２６】請求項３に対応する効果：請求項１及び２に対応する効果に加えて、演算処理手段の演算手法として、有効な実施化手段を提供することができる。

【００２７】請求項４，５に対応する効果：請求項１ないし３に対応する効果に加えて、演算処理手段の結果により辞書テーブルを参照しパスワードを得るための手法として有効な具体化手段を提供することができる。

【００２８】請求項６に対応する効果：請求項１ないし５に対応する効果に加えて、特徴の分析能力を高めることができ、認証の精度を上げることができる。

【００２９】請求項７に対応する効果：請求項１ないし６に対応する効果に加えて、文字・図形入力手段として有効な実施化手段を提供できる。

【００３０】請求項８に対応する効果：請求項１ないし７に対応する効果に加えて一般的な情報処理装置における認証に適応するだけではなく、通信システムのシステム要素を構成する情報処理装置に適用することによりネットワークへの負荷が減少し、通信システムに適した認証を行うことが可能となる。

【図面の簡単な説明】

【図１】本発明によるパスワード生成装置の一実施例の概要を示すブロック図である。

【図２】図１に示したブロック演算部において、特徴パラメータからパスワードパラメータへの変換の演算としてＭＤ５を用いる例を示す図である。

【図３】図１に示したパスワード生成部において行うパスワード生成のための処理の一例を示す図である。

【図４】パスワードパラメータによる数値列を参照値として文字辞書テーブルを利用し生成されるパスワードの例を示す図である。

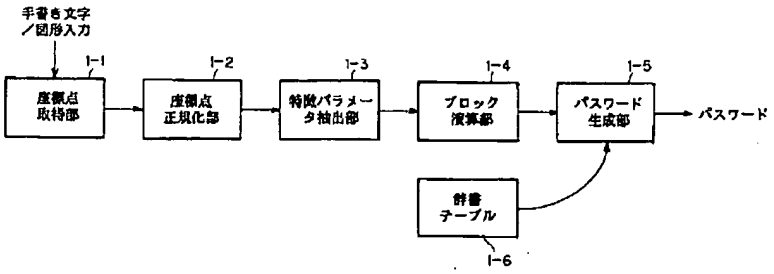
【図５】パスワードパラメータによる数値列を参照値として単語辞書テーブルを利用し生成されるパスワードの例を示す図である。

【図６】本発明の一実施例を示すブロック図である。

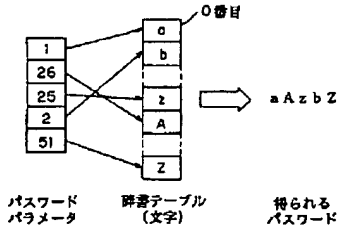
【符号の説明】

１－１…座標点取得部、１－２…座標点正規化部、１－３…特徴パラメータ抽出部、１－４…ブロック演算部、１－５…パスワード生成部、１－６…辞書テーブル、２－１，２－１′…１０２４ビットごとの切り出し、２－２，２－２′…ＭＤ５の計算、３－１，３－１′…１６ビットごとの切り出し、３－２，３－２′…辞書テーブル参照、３－３…英単語辞書テーブル。

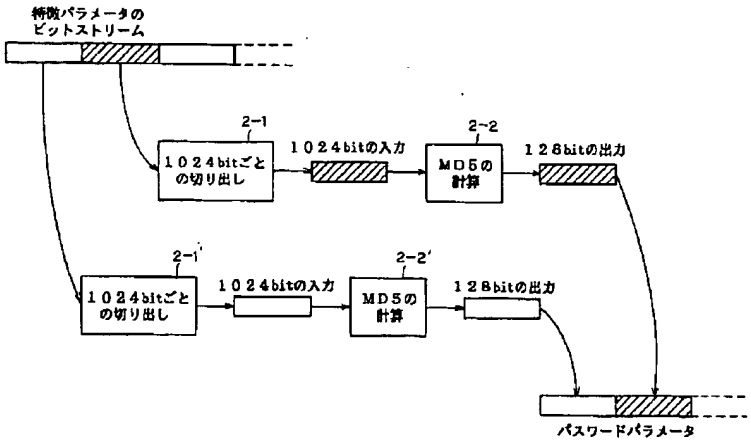
【図１】



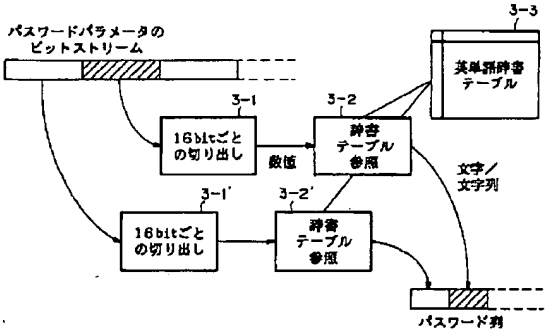
【図４】



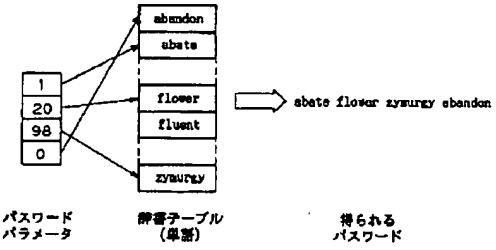
【図2】


特徴パラメータの
ビットストリーム
2-1
1024bitごと
の切り出し
1024bitの入力
2-2
MD5の
計算
128bitの出力
2-1'
1024bitごと
の切り出し
1024bitの入力
2-2'
MD5の
計算
128bitの出力
パスワードパラメータ

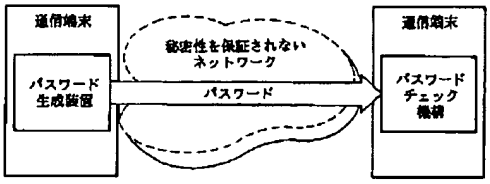
【図3】


パスワードパラメータの
ビットストリーム
3-3
英単語辞書
テーブル
3-1
16bitごと
の切り出し
3-2
辞書
テーブル
参照
数値
文字/
文字列
3-1'
16bitごと
の切り出し
3-2'
辞書
テーブル
参照
パスワード列

【図5】


1
20
98
0
abandon
abate
flower
fluent
zymurgy
abate flower zymurgy abandon
パスワード
パラメータ
辞書テーブル
(単語)
得られる
パスワード

【図6】


通信端末
パスワード
生成装置
秘密性を保証されない
ネットワーク
パスワード
通信端末
パスワード
チェック
機構